In an effort to explain some recent questions concerning GDOT's email system the following information is being sent for your benefit.

EMAIL STATISTICS:

During this past week of August 27 – August 31, GDOT's Virus and Spam preventing technology has scanned a total of 1,130,760 email messages.

Total messages scanned/processed: 1,130,760
Total messages identified as SPAM: 1,047,000
Total messages identified as VIRUS: 5,000

Total messages processed per minute   158
Total messages processed per day   226,152

The messages identified as SPAM and a VIRUS were never delivered to your inbox. These messages were captured by the system before delivery.

NEW SPAM ISSUES

The Office of Infrastructure is responsible for maintaining a secure and virus free email system while minimizing SPAM. In this effort, we have deployed several key technologies used to identify and filter out email messages that could be potentially harmful while trying to ensure every valid email is delivered. The creators of SPAM and viruses are constantly changing their techniques to get past the filters, which means we are updating our systems daily. Most recently (June 2007), a new SPAM campaign was launched in which spammers embed their messages within small PDF files. Because of this we have recently blocked emails which contain a PDF attachment that is less than 25K in size.   Legitimate PDF files are typically larger than the current filter size, so impact to users should be minimal.

In addition to a variety of scanning and filtering rules the following is a list of all attachment types that are blocked from delivery in GDOT's email system and the reasons why they are blocked.

Email Type Blocked	Purpose of Filter Block Rule
.exe, .com, .cab, .cmd, .pif, .rar, .scr, .vbe, .vbs, .fdf, .bat	Known to carry viruses
.zip	Known to carry viruses
.mp3 greater than 300k	Music files tend to be large and slow down mail delivery.
.pdf less than 25k	Causes large amounts of SPAM which are typically very small images embedded in PDF files

TIPS For Ensuring Successful Email Delivery:

- If you suspect an email containing a legitimate PDF or other file attachment listed above has been blocked, please contact the Solutions Center and someone will assist you with delivery.

- Ask the sender to change the file attachment extension before sending. You may also be required to change your file extension if you are trying to deliver a message externally. (example: testfile.pdf changed to testfile.pdf1) Once the recipient receives the email, they will simply rename the file using the correct extension. (testfile.pdf1 is renamed to testfile.pdf)

- If you continue to experience issues receiving legitimate email attachments, please submit your issues to the Solutions Center and our staff will be available to assist you.

- It's also important to remember there can be issues on the recipient's messaging system that will impact a successful delivery. Once an e-mail leaves our system, it is then subject to processing by the recipient's messaging system. There are times when a recipient's mail servers are not available. When this happens you will be notified that the message has been delayed, and if the recipients mail system comes back within 24 hours, your message will be delivered – if not, you will receive a non-delivery notice.

Please contact the Solutions Center at 404-651-5010 if you have any questions or concerns.